

**ONTARIO
SUPERIOR COURT OF JUSTICE**

B E T W E E N:

ZEXI LI

Plaintiff/Moving Party

and

CHRIS BARBER, BENJAMIN DICHTER, TAMARA LICH, PATRICK KING and
JOHN DOE 1, JOHN DOE 2, JOHN DOE 3, JOHN DOE 4, JOHN DOE 5,
JOHN DOE 6, JOHN DOE 7, JOHN DOE 8, JOHN DOE 9, JOHN DOE 10,
JOHN DOE 11, JOHN DOE 12, JOHN DOE 13, JOHN DOE 14, JOHN DOE 15,
JOHN DOE 16, JOHN DOE 17, JOHN DOE 18, JOHN DOE 19, JOHN DOE 20,
JOHN DOE 21, JOHN DOE 22, JOHN DOE 23, JOHN DOE 24, JOHN DOE 25,
JOHN DOE 26, JOHN DOE 27, JOHN DOE 28, JOHN DOE 29, JOHN DOE 30,
JOHN DOE 31, JOHN DOE 32, JOHN DOE 33, JOHN DOE 34, JOHN DOE 35,
JOHN DOE 36, JOHN DOE 37, JOHN DOE 38, JOHN DOE 39, JOHN DOE 40,
JOHN DOE 41, JOHN DOE 42, JOHN DOE 43, JOHN DOE 44, JOHN DOE 45,
JOHN DOE 46, JOHN DOE 47, JOHN DOE 48, JOHN DOE 49, JOHN DOE 50,
JOHN DOE 51, JOHN DOE 52, JOHN DOE 53, JOHN DOE 54, JOHN DOE 55,
JOHN DOE 56, JOHN DOE 57, JOHN DOE 58, JOHN DOE 59 and JOHN DOE 60

Defendants/Responding Parties

Proceeding under the *Class Proceedings Act, 1992*

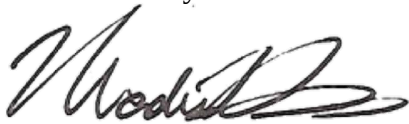
AFFIDAVIT OF RICH SANDERS

I, Rich Sanders, of the City of Pittsburgh, in the State of Pennsylvania, MAKE OATH
AND SAY:

1. I am a principal at CipherBlade Blockchain Investigation Agency. I provide professional services in the realms of blockchain forensics and cryptocurrency cybercrime investigation.
2. Attached as **Exhibit “A”** to this affidavit is my supplemental expert report in this matter dated February 16, 2022. I adopt the contents of that report as true.

3. In addition, attached as **Exhibit “B”** to this affidavit is a graph that I had intended to include with my initial report dated February 14, 2022, but which was inadvertently not included.

SWORN by Rich Sanders of the City of Pittsburgh, in the State of Pennsylvania, before me at the City of Toronto, in the Province of Ontario, on this 16th day of February, 2022, in accordance with O. Reg. 431/20, Administering Oath or Declaration Remotely.



Commissioner for Taking Affidavits
(or as may be)

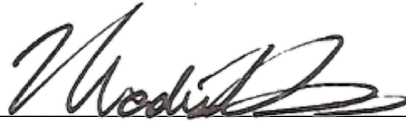
Madison Robins



Richard Sanders

(Signature of deponent)

This is Exhibit "A" referred to in the Affidavit of RICH SANDERS
sworn February 16, 2022.

A handwritten signature in black ink, appearing to read "Modest", is written over a horizontal line.

Commissioner for Taking Affidavits (or as may be)



CipherBlade

Blockchain Investigation Agency

SUPPLEMENTAL INVESTIGATIVE REPORT

Matter: Freedom Convoy

Date: February 16, 2022

Case: *Li v Barber et al*,
Court File No. CV-22-00088514-00CP

Background

1. I prepared a report on this matter dated February 14, 2022. I have been asked to address a number of questions in a supplemental report. The questions and the answers I have been asked to provide are set out below.

1) Where is cryptocurrency, like Bitcoin, located?

2. Bitcoin is a cryptocurrency that is contained in an online distributed ledger system, such as a blockchain. A blockchain is made up of blocks containing information that relates to transactions that take place on the blockchain, data such as; the date and time a transaction took place, the sending and receiving wallets, and the amount of cryptocurrency sent. As such, any particular user's Bitcoin does not exist in any physical location in any meaningful sense. To put it differently, if I own a Bitcoin, my Bitcoin is not located uniquely in any single jurisdiction. Rather, the information that indicates that I own that Bitcoin, is distributed on a database across the internet. In this way, cryptocurrency like Bitcoin can be analogized to representative currency, such as the type of currency that can be held in a bank account, though there are some differences (as described below).

Because Bitcoin ownership is reflected in a blockchain, there is no way to seize Bitcoin itself, in the sense of physically going and taking an object like cash (i.e. fiat currency). However, there are physical wallets which contain the private keys required to access the Bitcoin. Some specific examples are; 1) "paper wallets"¹ of which are physical pieces of paper, which contain the seed words, or the private keys that are necessary to access the wallet containing the Bitcoin; 2) Physical devices such as "OpenDime's"² which operate as a read-only USB flash drives that effectively contain a Bitcoin wallet, they can be used to receive Bitcoin, be passed on from person to person, and then unsealed revealing the private key that can then be used to spend the Bitcoin. Similarly, because the Bitcoin blockchain is a decentralized system, there is no practical way that a centralized authority can transfer the Bitcoin from one person to another, like a bank transferring representative currency in a bank account. Put simply, there is no central Bitcoin authority (like a bank) who can be directed to transfer ownership of particular Bitcoin from one person to another; that is not how blockchains work.

3. However, that does not mean that it is impossible for Courts and other legal authorities to make orders that have the effect of freezing or seizing Bitcoin. To the contrary, based on my prior experience in these types of matters, it is common for courts to make orders that have the effect of freezing or seizing Bitcoin.

¹ <https://bitcoinpaperwallet.com/>

² <https://opendime.com/>

4. As I explained in my initial report, a Bitcoin wallet and its associated credentials are always controlled by one or more individuals or by companies. It is that wallet, and those credentials, which control what happens to that particular Bitcoin.

5. There are at least two distinct mechanisms by which a Court order can result in the freezing or seizure of Bitcoin. To help conceptualize what each of these means, I will also provide analogies to how this would work with fiat currency.

6. First, a Court could order a particular individual who knows the credentials to the associated Bitcoin or cryptocurrency wallet, to either a) not transfer their Bitcoin to anyone else; or b) transfer their Bitcoin to a third-party to be held by them. The first is directly analogous to a Court order directing an individual who holds cash in their wallet or at their home to not transfer it to anyone else, while the second is directly analogous to a Court order directing an individual who holds cash in their wallet or at their home to provide the funds to a third-party. Conceptually, the Court's order is effectively identical with respect to both Bitcoin and fiat currency: the only difference is in the subject matter. With fiat currency, the order restricts or requires actions by a particular individual with respect to a physical object, cash. With Bitcoin, the order restricts or requires actions by an individual with respect to a digital asset, Bitcoin held in their wallet, using their credentials. In both cases, the order is directed at an individual and what they can or cannot do.

7. The only difference between an order requiring someone to take particular steps with respect to cash and an order requiring someone to take particular steps with respect to Bitcoin is that an order with respect to Bitcoin can be more easily monitored and enforced. If an order is made against a person directing them not to dispose of any cash they hold, it is difficult to monitor compliance if the person were to deliberately try to evade a Court order. For example, if I were an unscrupulous person and I got notice of that order, I might immediately try to hide my cash or give it to a similarly unscrupulous friend for safekeeping. If no one knew that I had the cash in the first place, they would never know I had transferred it. Even if they did know I had the cash in the first place, they might have no idea to whom I transferred it.

8. By contrast, with Bitcoin, there is a high degree of visibility. All Bitcoin transactions are publicly visible to anyone on the Bitcoin blockchain. In practice, that means that if you know that a particular person controls Bitcoin in a particular wallet, it is possible to determine: a) whether the Bitcoin is transferred to anyone else; b) which wallet it is transferred to; and c) when it is transferred. Consequently, orders requiring persons to either deal in a particular way or not deal in Bitcoin are in this way more enforceable than orders pertaining to cash due to the aforementioned reasons.

9. The second way that a Court order could effectively result in a freezing or seizure of Bitcoin relates to cryptocurrency exchanges. As I described in my first report, a cryptocurrency exchange

is essentially a way to effect transactions for cryptocurrency. In order to transfer one form of cryptocurrency into a different form (such as an alternative cryptocurrency or non-fungible token, or into a non-digital form such as a gift card or fiat money), cryptocurrency is processed through an exchange. During the transaction, the individual must temporarily cede control over their Bitcoin to the exchange (much as one effectively cedes control over one's fiat money to a bank when making a deposit. If I were to deposit a \$100 note to the bank, I am effectively ceding control of that \$100 note and in return, I receive a ledger entry in the bank account – exchanges function the same way, it is effectively an IOU). Because cryptocurrency is held in a wallet with a unique identifier, a Court order could order a cryptocurrency exchange not to permit transactions involving particular wallets and/or to either freeze an individual's cryptocurrency holdings (in their exchange account) or transfer their holdings to someone else.

10. Again, there is little conceptual difference between how an order would be directed against a bank holding representative currency and a cryptocurrency exchange holding Bitcoin. In both cases, the Court order is directed against the party holding the funds, requiring them to do or not do particular things.

11. In the case of a bank holding representative currency, when an individual makes a deposit, the bank does not actually hold all of its depositors' money in a box, waiting for them to be paid. Rather, the bank takes depositors' money and puts it to other uses; however, the bank is subject to a legal obligation to transfer the funds back to the depositor on request. A freezing order against a bank therefore does not actually freeze any physical money; rather, it merely tells the bank to maintain certain obligations in a certain manner and to not let people modify them. Similarly, where an order is directed against a cryptocurrency exchange, it tells them not to allow any transactions pertaining to particular addresses or accounts.

12. In summary, while there is no physical Bitcoin asset that can be frozen or seized, Court orders can be and are routinely made against persons and entities that control Bitcoin. While Bitcoin does not have any physical existence (like cash), it does exist in terms of accounting entries (like representative currency in the form of deposits in a bank).

2) Can Bitcoin be transferred directly to other wallets without going through an exchange?

13. Yes, Bitcoin can be transferred directly from one Bitcoin wallet to another Bitcoin wallet without going through an exchange. However, as noted in my previous report, transfers of Bitcoin are recorded in the blockchain and are viewable, for free, by anyone. This means that movement of Bitcoin from one wallet to another can be easily monitored.

3) Are there persons within Ontario who could be subject to an order of an Ontario court pertaining to their Bitcoin? If so, explain how.

14. For the purpose of answering this question, I have been asked to assume that Ontario court

orders are enforceable against persons physically present in Ontario and companies that are physically present or carry on business in Ontario. With that assumption made, assuming that there are persons or companies that control particular Bitcoin within Ontario, those persons in Ontario that could be the subject of an Ontario court order.

15. As I explained above, an individual's Bitcoin does not reside in any particular location. However, as I explained above, control over Bitcoin is determined by the person who controls the Bitcoin wallet. Consequently, a Court will control over the location of Bitcoin if it has jurisdiction over the individual who controls the Bitcoin wallet. Put simply, if I were located in Ontario, and an Ontario court validly issued orders to me (under threat of various penalties), it could order me to take particular steps with respect to my Bitcoin.

16. In this case, I understand that members of the Freedom Convoy are protesting in Ottawa, Ontario. Assuming that the individuals who control any Bitcoin wallets are located in Ontario, and based on the other assumptions I have been provided above, the Ontario court will be to render orders against individuals in respect of their Bitcoin holdings that are enforceable in Ontario. (In answering this question, I note that I am not a lawyer, and my opinion is expressly based on the assumptions I have provided above about the circumstances in which an order will be enforceable in Ontario)

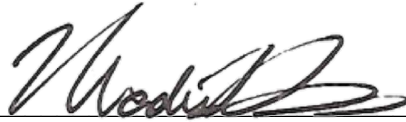
17. In addition, as I noted in my first report, there are a number of cryptocurrency exchanges that operate in Canada, and some of those operate in Ontario in particular. For example, the website of Bitbuy, one Canadian cryptocurrency exchange, indicates that its mailing address is in Toronto, Ontario. Based on the assumption I have been asked to make that a business can be subject to an Ontario court order if they are physically present in Ontario, Bitbuy could be subject to an Ontario court order.

18. In respect of cryptocurrency exchanges that are located outside of Canada, I cannot comment on whether an Ontario court order could be enforced against them, because that falls outside my area of expertise. However, I can say that the scenario would be analogous to trying to enforce an Ontario court order against a foreign bank located outside of Ontario.

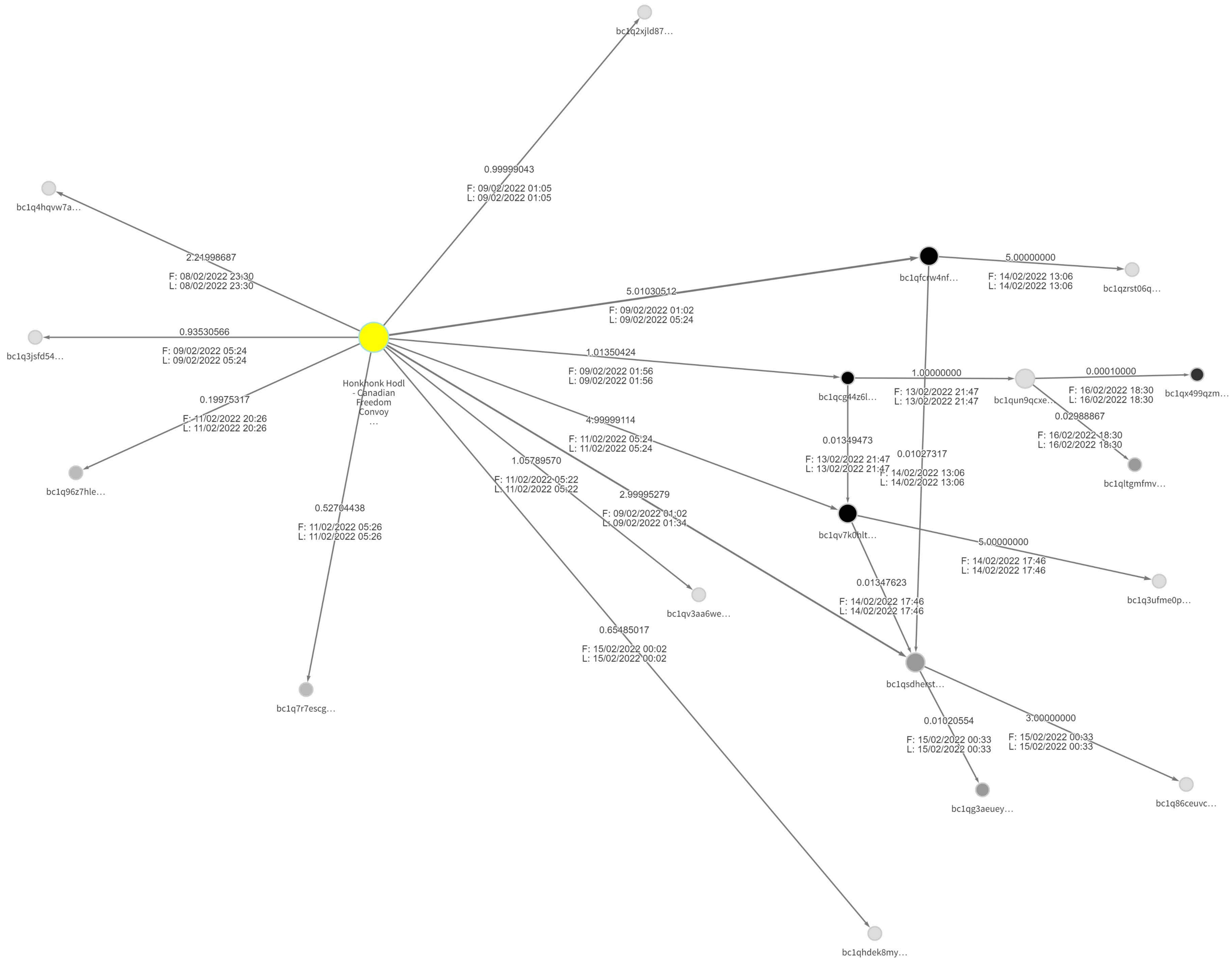
Subscribed to before me
by RICHARD SANDERS, CRC, CISC
this 16th day of February, 2022.


Richard A. Sanders
Lead Investigator, Principal
CipherBlade

This is Exhibit "B" referred to in the Affidavit of RICH SANDERS
sworn February 16, 2022.

A handwritten signature in dark ink, appearing to read "Modest", is written over a horizontal line.

Commissioner for Taking Affidavits (or as may be)



ZEXI LI.
Plaintiff (Moving Party)

-and- CHRIS BARBER et al.
Defendants (Responding Parties)

Court File No. CV-22-00088514-00CP

ONTARIO
SUPERIOR COURT OF JUSTICE
PROCEEDING COMMENCED AT OTTAWA

AFFIDAVIT OF RICH SANDERS

LENCZNER SLAGHT LLP

Barristers
Suite 2600
130 Adelaide Street West
Toronto ON M5H 3P5

Monique J. Jilesen

Tel:

Email:

Madison Robins

Tel:

Email:

Sarah Bittman

Tel:

Email:

Acting as Agent to Champ & Associates, Counsel for
the Plaintiff, Zexi Li